DIGITAL WATERMARKING FOR MEDICAL IMAGE AUTHENTICATION

NOOR AQILAH BINTI ABDUL HALIM

BACHELOR OF COMPUTER SCIENCE

UNIVERSITI MALAYSIA PAHANG

Universiti Malaysia PAHANG

SUPERVISOR'S DECLARATION

I hereby declare that I have checked this thesis and in my opinion, this thesis is adequate in terms of scope and quality for the award of the degree of Computer Science in Graphic and Multimedia Technology

(Supervisor's Signature)

Full Name : Dr. Ferda Ernawan

Position : Senior Lecturer

Date : 9th January 2019

Universiti Malaysia PAHANG

STUDENT'S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citations which have been fully acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Universiti Malaysia Pahang or any other institutions.

(Student's Signature)

Full Name : Noor Aqilah Binti Abdul Halim

ID Number : CD15054

DIGITAL WATERMARKING FOR MEDICAL IMAGE AUTHENTICATION

NOOR AQILAH BINTI ABDUL HALIM

Thesis submitted in fulfillment of the requirements for the award of the degree of Bachelor of Computer Science (Graphics & Multimedia Technology)

Faculty of Computer Systems & Software Engineering
UNIVERSITY MALAYSIA PAHANG

JANUARY 2019

ACKNOWLEDGEMENTS

Upon completing this thesis, I was in many contacts with many people, researchers and academicians. They have contributes so much towards improving my understanding in this field. In particular, I wish to express my greatest gratitude to my thesis supervisor, Dr. Ferda Ernawan. Without his continued advice, support and guidance, this thesis wouldn't possibly be able to be completed as presented. Special thanks to Dr. Liew Siau Chuin who was so kind to share with me his previous research content that had helped me develop an improve method from his previous scheme.

I would like to thank my Final Year Project coordinator, Sir Mohd Arfian bin Ismail and Faculty of Computer Systems & Software Engineering of Universiti Malaysia Pahang for providing the needed resources, information, and knowledge required to complete my thesis.

I would like to thank my family and friends who have supported and motivated me whenever I needed it. Lastly, I would like to apologize to those I might have missed out to mention who had helped me throughout the process of completing this thesis.

ABSTRAK

Pengaruh imej digital dalam bidang perubatan telah membawa impak pada masa kini. Walau bagaimanapun, dengan peningkatan penggunaan imej perubatan dalam bentuk digital, turut meningkat potensi imej untuk terdedah kepada ancaman diubahsuai. Oleh itu, amatlah penting agar imej perubatan dilindungi daripada sebarang kerosakan. Watermarking digital sangat sesuai untuk diunakan dalam situasi ini. Tujuan penyelidikan ini adalah untuk mencadangkan kaedah penambahbaikan bagi pengesahan keaslian imej perubatan. Imej watermark akan dimasukkan ke dalam imej perubatan dengan menggunakan skema watermarking yang rapuh. Selepas itu, imej yang diagihkan akan diuji dengan pelbagai jenis ancaman seperti potongan dan pemampatan sebelum watermark tersebut diekstrak dari imej perubatan untuk memeriksa keasliannya. Watermarking yang boleh diterbalikkan memberikan mampu mengesahkan imej asal dan dapatkan kembali watermark yang telah ditanam. Untuk kajian ini, skema watermarking yang rapuh dijangka akan memastikan watermark yang tertanam akan musnah dengan mudah jika imej watermarked mengalami sedikit pengubahsuaian untuk membuktikan kesahihan imej perubatan. Ini akan membantu membuktikan kesahihan imej perubatan.

ABSTRACT

The influence of digital image in the fields of medical line had become a major impact nowadays. However, with the increasing use of medical image in digital form, so does the potential of the image to be exposed to threat of being modified. Therefore, it is crucial for the medical image to be protected from unauthorized usage. Digital watermarking serves well for this situation. The aim of this research is to propose an improve method for watermarking authentication of medical image. Watermark image will be embedded into the medical image by using fragile watermarking schemes. Afterwards, the watermarked medical image will be tested with various type of threat such as cropping and compression before the watermark is extracted back from the watermarked medical image to inspect its' authenticity. Reversible Watermarking provides the authentication that can retrieve the original image and the watermark. For this research, fragile watermarking is projected where the method of operation is to let the embedded watermark to be destroyed easily if the watermarked image undergoes even slight modification in order to prove the authenticity of the medical image. This will help in proving authenticity of medical images.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

NROI	Non Region of Interest
ROI	Region of Interest
RLE	Run-length Encoding
LSB	Least Significant Bit
RONI	Region of Non Interest

CHAPTER 1

INTRODUCTION

1.0 INTRODUCTION

Nowadays, digital media have evolved the way still image are used, stored and transmitted, allowing growth to a wide range of new application that are expected to make an important impact on the multimedia industry. One of the advantages of digital multimedia is the ease of accessed, manipulation and duplication (Rippa & Secundo, 2018). However, this feature brought a major side effect since it causes unauthorized alteration of information such as data piracy. Hence, intellectual property rights protection of stored and transmitted images is a very important concern (Khanduja, 2017). Watermarking is a great way to help protecting the property rights of digital media. Digital watermarking is a process of embedding data into digital multimedia contents (Techopedia Inc, 2018). It can prove the originality of the content or to verify the identity of the digital content's owner.

Robust watermarking has a main goal which even when the watermarked image endures accidental or purpose attacks, the watermark embedded in the original image will be unaffected and can be extracted and identified (Pramila, Keskinarkaus, & Seppänen, 2018). Therefore, it is suitable for ownership verification. Meanwhile, fragile watermarking is used to verify the authenticity and integrity of digital images (Renza, L., & Lemus, 2018). Fragile watermarking can help prove the authenticity of medical image by proving the presence of tamper and mark it (Hisham, Muhammad, Badshah, Johari, & Zain, 2017).

1.1 EXISTING METHOD FOR IMAGE AUTHENTICATION

Previously, a few methods had been proposed for fragile watermarking to be used for medical image authentication. A dual watermarking method was proposed by Qiang and Hongbin for tamper detection and self-recovery by embedding the watermark data in two regions, which are in least significant bit (LSB) and the discrete wavelet transform (DWT) of the host image. The objective is to make sure that if any alteration occurs to at LSB, the data is still safely secured in DWT for the recovery process (Song & Zhang, 2010). The scheme proposed by (Bravo-Solorio & Nandi, 2011) has been suggested which integrating two methods to strengthen the tampering localization ability, which are a secure block-wise resilient to cropping mechanism and an iterative pixel-wise mechanism. It is said that this method manages to prevent cropping attack (Bravo-Solorio & Nandi, 2011). Block-based mechanism is a famous method for fragile watermarking. The researchers (Lin, Yang, & Xu, 2011)also used block-based mechanism for tampering detection, but the focus is on colour image. The algorithm has two main steps to locate any tampered region, which are a rough judgment and an accurate judgment step (Lin, Yang, & Xu, 2011). Another scheme for authentication proposed, involve the approach of RONI and ROI. The embedding locations for the watermarking bits are based on a chaotic key (Nasseem, Qureshi, Atta-ur-Rahman, & Muzaffar, 2013).

Image watermarking for medical image authentication focus more on determine whether the medical image authenticity is proven or not (Arsalan, Qureshi, Khan, & Rajarajan, 2017). Although the recovery feature is very helpful for the doctors to easily know whether the image is authentic or not but the most crucial process is to determine the validity of the image, whether any attack is performed or not and whether the manipulation could bring harms or misleading to the diagnosis. Therefore, the research will not cover on recovery of the altered medical image.

The numbering with spiral pattern method is not suitable for rectangular images. The scheme could only be embedded onto the square part of the centre and will leave the top and bottom uncovered from watermark thus making the result very promising when the tamper occurs only on the watermark region (Hisham, Muhammad, Badshah, Johari, & Zain, 2017). Hence it becomes a flaw to this method as it did could not perform well in non-square images while it is a norm since most medical images are produces or scanned in rectangle shape.

The objective of this research is to propose a more secure method to be used for medical image authentication. Thus, by comparing three methods from previous research, the advantages and drawback of implementing each method will be discuss.

1.2 RESEARCH QUESTION

Q1: What is the suitable watermark embedding technique for medical image authentication?

This research question asks about the suitable watermarking scheme to be used to test the medical image authenticity. The embedding scheme used must be convenient to help detecting if there is any alteration done on the medical image. The watermarking scheme use should be fragile against any attack to ensure that the medical image authenticity can be proven when there is no alteration detected due to the watermark not destroyed. The watermarking scheme should not cause the medical image to lose its' quality.

Q2: How can we locate modified part of the medical image to test its' authenticity?

This research question proposed that the process to locate the altered part is important to test the authenticity of medical image. The slightest change or alteration should be able to be recognized on the medical image.

Q3: How can we evaluate the performance of watermarking for medical image authentication method?

This research question asks about the best way to verify the performance of the each method for medical image authentication. There is a lot of existing method for image authentication which can be made as a reference on evaluation of the best authentication detection for medical image.

1.3 RESEARCH PROBLEM

Table 1.3 Research Problems

Problem	**Description**	**Effect**
The TALLOR embedded the watermark in a sequence order in selected Region of Non Interest (RONI). (Zain S.-C. L., 2011)	The embedded data coordinate is easily detected and replaced with new data.	Image is falsely detected as authentic.

REFERENCES

Al-Qershi OM, K. B. (2011). *Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images.*

Ankita Vaish, M. K. (2017). Color image encryption using MSVD, DWT and Arnold transform in fractional Fourier domain. *Optik Volume 145*, 273-283.

Arsalan, M., Qureshi, A. S., Khan, A., & Rajarajan, M. (2017). Protection of medical images and patient related information in healthcare: Using an intelligent and reversible watermarking technique. *Applied Soft Computing*, 168-179.

Bravo-Solorio, S., & Nandi, A. K. (2011). Secure fragile watermarking method for image authentication with improved tampering localisation and self-recovery capabilities. In S. Bravo-Solorio, & A. K. Nandi, *Signal Processing*, 728-739.

Harase, S. (2018). Conversion of Mersenne Twister to double-precision floating-point numbers. *Mathematics and Computers in Simulation*.

Hisham, S. I., Liew, S.-C., & Zain1, J. M. (2013). A Quick Glance at DigitalWatermarking in Medical Images. *Biomedical Engineering Research*, 79–87.

Hisham, S. I., Muhammad, A. N., Badshah, G., Johari, N. H., & Zain, J. M. (2017). *Numbering with spiral pattern to prove authenticity and integrity.*

Khanduja, V. (2017). Database watermarking, a technological protective measure: Perspective, security analysis and future directions. *Journal of Information Security and Applications*, 38-49.

Kumar, J., Singh, P., A.K.Yadav, & Kumar, A. (2018). Asymmetric Cryptosystem for Phase Images in Fractional Fourier Domain Using LU-Decomposition and Arnold Transform. *Procedia Computer Science*, 1570-1577.

Lin, H., Yang, S., & Xu, L. (2011). Watermark algorithm for color image authentication and restoration. *Proceedings of 2011 International Conference on Electronic & Mechanical Engineering and Information Technology*, 2773–2776.

Nasseem, M. T., Qureshi, I. M., Atta-ur-Rahman, & Muzaffar, M. Z. (2013). Chaos based invertible authentication of medical images. *2013 IEEE 9th International Conference on Emerging Technologies (ICET)*, 1-5.

PhoolSingh, A.K.Yadav, & KeharSingh. (2017). Phase image encryption in the fractional Hartley domain using Arnold transform and singular value decomposition. *Optics and Lasers in Engineering*, 187-195.

Pramila, A., Keskinarkaus, A., & Seppänen, T. (2018). Increasing the capturing angle in print-cam robust watermarking. *Journal of Systems and Software*, 205-215.

Renza, D., L., D. M., & Lemus, C. (2018). Authenticity verification of audio signals based on fragile watermarking for audio forensics. *Expert Systems with Application*, 211-222.

Rippa, P., & Secundo, G. (2018). Digital academic entrepreneurship: The potential of digital technologies on academic entrepreneurship. *Technological Forecasting and Social Change*.

Saito, M., & Matsumoto, M. (2006). SIMD-Oriented Fast Mersenne Twister: a 128-bit Pseudorandom Number Generator. *Monte Carlo and Quasi-Monte Carlo Methods*, 607-622.

Siau-Chuin Liew, J. M. (2012). Tamper Localization and Lossless Recovery Watermarking Scheme with ROI. *Journal of Digital Imaging*, 316-325.

Song, Q., & Zhang, H. (2010). Image Tamper Detection and Recovery Using Dual Watermark. *2010 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM).* Chengdu, China: IEEE.

Techopedia Inc. (2018). *What Is Digital Watermarking? - Definition from Techopedia*. Retrieved March 21, 2018, from Techopedia.com: https://www.techopedia.com/definition/24927/digital-watermarking

Vilardy, J. M., Torres, C. O., & Jimenez, C. J. (2013). *Double image encryption method using the Arnold transform in the fractional Hartley domain.*

Zain, J. M., & ARM, F. (2006). Medical image watermarking with tamper detection and recovery. *The 28th annual international conference of the IEEE Engineering in Medicine and Biology Society.* New York, USA: IEEE.

Zain, J., Baldwin, L., & Clarke, M. (2004). Reversible watermarking for authentication of DICOM images. *Proceedings of 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, 3237-3240.

Zain, S.-C. L. (2011). Tamper Localization and Lossless Recovery Watermarking Scheme. *Communications in Computer and Information Science book series*, 555-566.

Zheng, L., Zhang, Y., & Thing, V. L. (2018). A Survey on Image Tampering and Its Detection in Real-world Photos. *Journal of Visual Communication and Image Representation*.

ZHou, X., Huang, H., & Lou, S. (2001). Authenticity and integrity of digital mammography images. *IEEE Transactions on Medical Imaging*, 748-791.